Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended): A system for providing telephonic content security service in a wireless network environment, comprising:

a plurality of wireless devices interfacing over a network providing wireless telephonic services through a layered service architecture;

a status daemon periodically communicating operational data from each wireless device to the network operations center, said operational data being in the form of a report on status and health of the wireless device;

a provisioning framework provisioning content security services to the wireless devices via the layered service architecture, each content security service delivered through applications executing in a user layer on each wireless device, comprising:

a network operations center supervising the provisioning of the content security services to each wireless device and maintaining a master catalog of the applications and further maintaining a configured wireless devices list reflecting the status of each wireless device based on the operational data; and

a configuration client managing a configuration of each wireless device by consulting the master catalog and the configured wireless devices list and downloading the applications to each wireless device as required to maintain each wireless device in a most-up-to-date configuration; and

each wireless device delivering the content security services as functionality provided through execution of the applications.

2. (currently amended): A system according to Claim 2~~, further comprising:~~

a wherein said status daemon periodically ~~pushing~~ pushes the operational data from each wireless device to the network operations center.

3. (currently amended): A system according to Claim 2~~, further comprising:~~

~~a~~ wherein said status daemon ~~pulling~~ pulls the operational data from each wireless device to the network operations center on-demand.

4. (currently amended): A system according to Claim [[2]] 1, further comprising:

a reporting module creating at least one of an informational report and a statistics report from the operational data.

5. (currently amended): A system according to Claim [[2]] 1, further comprising:

a reporting module generating an alert from the operational data upon detecting a faulty wireless device.

Claims 6-8 (canceled).

9. (original): A system according to Claim 1, further comprising:

an application repository maintained on a remote component server storing the applications under control of the network operations center.

10. (original): A system according to Claim 1, further comprising:

a local application repository maintained on a local component server storing the applications under control of the network operations center.

11. (original): A system according to Claim 1, wherein the content security service comprises antivirus scanning and the application comprises an antivirus scanner.

12. (currently amended): A method for providing telephonic content security service in a wireless network environment, comprising:

interfacing to a plurality of wireless devices over a network providing wireless telephonic services through a layered service architecture;

periodically communicating operational data from each wireless device to the network operations center using a status daemon, said operational data being in the form of a report on status and health of the wireless device;

provisioning content security services to the wireless devices via the layered service architecture, each content security service delivered through applications executing in a user layer on each wireless device, comprising:

supervising the provisioning of the content security services to each wireless device from a network operations center at which are maintained a master catalog of the applications and configured wireless devices list reflecting the status of each wireless device based on the operational data; and

managing a configuration of each wireless device from a configuration client by consulting the master catalog and the configured wireless devices list and downloading the applications to each wireless device as required to maintain each wireless device in a most-up-to-date configuration; and

delivering the content security services as functionality provided through execution of the applications on each wireless device.

13. (currently amended) A method according to Claim 12, wherein said step of periodically communicating operational data from each wireless device to the network operations center includes the step of ~~further comprising:~~

periodically pushing operational data from each wireless device to the network operations center.

14. (currently amended): A method according to Claim 12, wherein said step of periodically communicating operational data from each wireless device to the network operations center includes the step of ~~further comprising:~~

pulling operational data from each wireless device to the network operations center on-demand.

15. (currently amended): A method according to Claim [[~~13~~]] 12, further comprising:

creating at least one of an informational report and a statistics report from the operational data.

16. (currently amended): A method according to Claim [[~~13~~]] 12, further comprising:

generating an alert from the operational data upon detecting a faulty wireless device.

Claims 17-19 (canceled).

20. (original): A method according to Claim 12, further comprising:

maintaining an application repository on a remote component server storing the applications under control of the network operations center.

21. (original): A method according to Claim 12, further comprising:

maintaining a local application repository on a local component server storing the applications under control of the network operations center.

22. (original): A method according to Claim 12, wherein the content security service comprises antivirus scanning and the application comprises an antivirus scanner.

23. (currently amended): A computer-readable storage medium holding code for performing the method according to Claims 12, 13, 14, 15, 16, ~~17, 18, 19~~, 20, 21, or 22.

24. (currently amended): A system for provisioning a plurality of wireless devices in a closed content security service loop framework, comprising:

a wireless network environment comprising a plurality of wireless devices, each providing wireless telephonic services;

a centralized database comprising catalogs of configuration information for the wireless devices;

a configuration client determining the content security service components required for content security service delivery from the configuration information catalogs and providing the content security service components to each wireless device for configuration and execution; and

a network operations center delivering content security services to each wireless device through the content security service components being executed thereon, and automatically periodically receiving a status report from each wireless device by means of a status daemon, each status report providing status information comprising machine-specific data and application-specific information.

25. (original): A system according to Claim 24, further comprising:

an applet executing on the configuration client broadcasting a query message to one or more unconfigured wireless devices and receiving configuration requests from each unconfigured wireless device.

26. (original): A system according to Claim 24, further comprising:

a catalog server generating a catalog of out-of-date content security service components on each wireless device.

27. (original): A system according to Claim 24, further comprising:

an applet executing on the configuration client updating the out-of-date content security service components on each wireless device.

28. (original): A system according to Claim 24, further comprising:

a component server staging the content security service components.

29. (original): A system according to Claim 28, further comprising:

a network operations center storing the staged content security service components.

30. (original): A system according to Claim 28, further comprising:

at least one of a remote component server and a local component server storing the staged content security service components.

31. (original): A system according to Claim 24, further comprising:

a Web browser executing an applet on the configuration client to manage the configuration of the content security service components on each wireless device.

32. (currently amended): A method for provisioning a plurality of wireless devices in a closed content security service loop framework, comprising:

providing a wireless network environment comprising a plurality of wireless devices, each providing wireless telephonic services;

maintaining a centralized database comprising catalogs of configuration information for the wireless devices;

determining the content security service components required for content security service delivery from the configuration information catalogs and providing the content security service components to each wireless device for configuration and execution;

delivering content security services to each wireless device through the content security service components being executed thereon; and

automatically periodically receiving a status report from each wireless device by means of a status daemon, each said status report providing status information comprising machine-specific data and application-specific information.

33. (original): A method according to Claim 32, further comprising:

broadcasting a query message to one or more unconfigured wireless devices; and

receiving configuration requests from each unconfigured wireless device.

34. (original): A method according to Claim 32, further comprising:

generating a catalog of out-of-date content security service components on each wireless device.

35. (original): A method according to Claim 32, further comprising:

updating the out-of-date content security service components on each wireless device.

36. (original): A method according to Claim 32, further comprising:

staging the content security service components on a component server.

37. (original): A method according to Claim 36, further comprising:

storing the staged content security service components on a network operations center.

38. (original): A method according to Claim 36, further comprising:

storing the staged content security service components on at least one of a remote component server and a local component server.

39. (original): A method according to Claim 32, further comprising:

executing an applet configuration client on a Web browser to manage the configuration of the content security service components on each wireless device.

40. (original): A computer-readable storage medium holding code for performing the method according to Claims 32, 33, 34, 35, 36, 37, 38, or 39.